Efficient Transmission of Information on the Quantum Network(New Trends in Theory of Computation and Algorithm)

AUTHOR(S):

HAYASHI, MASAHITO; IWAMA, KAZUO; NISHIMURA, HARUMICHI; レイモンド, ルディー; 山下, 茂

CITATION:

HAYASHI, MASAHITO ...[et al]. Efficient Transmission of Information on the Quantum Network(New Trends in Theory of Computation and Algorithm). 数理解析研究所講究録 2006, 1489: 128-134

ISSUE DATE:

2006-05

URL:

http://hdl.handle.net/2433/58218

数理解析研究所講究録
1489巻 2006年 128-134

Efficient Transmission of Information on the Quantum Network
量子ネットワーク上での効率的な情報の伝送

MASAHITO HAYASHI[1] KAZUO IWAMA[2] HARUMICHI NISHIMURA[2]
RUDY RAYMOND[2] SHIGERU YAMASHITA[3]
林 正人 岩間 一雄 西村 治道 ルディーレイモンド 山下 茂

[1]ERATO-SORST Quantum Computation and Information Project,
Japan Science and Technology Agency
ERATO-SORST 量子情報システムアーキテクチャ
masahito@qci.jst.go.jp
[2]Graduate School of Informatics, Kyoto University 京都大学情報学研究科
{iwama, hnishimura, raymond}@kuis.kyoto-u.ac.jp
[3]Graduate School of Information Science, Nara Institute of Science and Technology
奈良先端科学技術大学情報科学
ger@is.naist.jp

Abstract. Since quantum information is continuous, its handling is sometimes surprisingly harder than the classical counterpart. A typical example is cloning; making a copy of digital information is straightforward but it is not possible exactly for quantum information. The question in this paper is whether or not *quantum* network coding is possible. Its classical counterpart is another good example to show that digital information flow can be done much more efficiently than conventional (say, liquid) flow.

Our answer to the question is similar to the case of cloning, namely, it is shown that quantum network coding is possible if approximation is allowed, by using a simple network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. Our results for quantum network coding include: (i) We can send any quantum state $|\psi_1\rangle$ from s_1 to t_1 and $|\psi_2\rangle$ from s_2 to t_2 simultaneously with a fidelity strictly greater than 1/2. (ii) If one of $|\psi_1\rangle$ and $|\psi_2\rangle$ is classical, then the fidelity can be improved to 2/3. (iii) Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states. This allows us to design an interesting protocol which can send two classical bits from s_1 to t_1 (similarly from s_2 to t_2) but only one of them should be recovered.

1 Introduction

Coding is obviously one of the most important techniques for information processing, and is used for many different purposes including cryptography, error correction, data compression, etc. Recently it has been shown that coding is also useful to effectively achieve larger channel capacity than can be achieved by simple routing. The technique is based on a completely different idea from data compression and has been known as *network coding* since its introduction by Ahlswede, Cai, Li and Yeung [2]. It has been quite popular as a mutual interest of theoretical computer science and information theory (see e.g., [14, 16, 17, 18] for recent developments).

Network coding is nicely explained by using the so-called Butterfly network as shown in Fig. 1. The capacity of each directed link is all one and there are two source-sink pairs s_1 to t_1 and s_2 to t_2. Notice that both paths have to use the single link from s_0 to t_0 and hence the total

amount of flow in both paths is bounded by one, say, 1/2 for each. Interestingly, this max-flow min-cut theorem no longer applies for "digital information flow." As shown in Fig. 2, we can transmit two bits, x and y, on the two paths simultaneously. Tricks here are (at least) twofold: The first one is the EX-OR (Exclusive-OR) operation at node s_0. One can see that the bit y is encoded by using x as a key which is sent directly from s_1 to t_2, and vise versa. The second trick is even more important; at node t_0 we can make an exact copy of one-bit information from s_0.

The main objective of this paper is to develop similar, but approximated network coding for *quantum* channels and *quantum* information. (It turns out that exact transmission is not possible, which one intuitively expects by the continuous nature of quantum information, the no-cloning theorem [23] etc.) For given two quantum states $|\psi_1\rangle$ at s_1 and $|\psi_2\rangle$ at s_2, our task is to transmit them to t_1 and t_2 simultaneously and output as $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$, respectively. Our goal is to make $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ as similar to the original $|\psi_1\rangle$ and $|\psi_2\rangle$ as possible, respectively (we use bold fonts for 2×2 and 4×4 density matrices for exposition). Every channel capacity remains one and any physically implementable operation is allowed at each node.

The key seems to be whether we can find tricks similar to the above classical case. For the second one, we may be able to use the approximated cloning by Bužek and Hillery [9], but for the first one, there is no obvious way of encoding a quantum state by a quantum state. Consider, for example, a simple extension of the classical operation at node s_0 by using a controlled unitary transform U as illustrated in Fig. 3. (Note that classical EX-OR is realized by setting $U = X$ "bit-flip.") Then, for any U, there is a quantum state $|\phi\rangle$ (actually an eigenvector of U) such that $|\phi\rangle$ and $U|\phi\rangle$ are identical (up to a global phase). Namely, if $|\psi_2\rangle = |\phi\rangle$, then $\boldsymbol{\rho}_1 = |\phi\rangle\langle\phi|$ at t_1 does not change for $|\psi_1\rangle = |0\rangle$ and $|\psi_1\rangle = |1\rangle$. Since $|0\rangle$ and $|1\rangle$ are orthogonal, this means either $|0\rangle$ and $\boldsymbol{\rho}_1$ or $|1\rangle$ and $\boldsymbol{\rho}_1$ are completely dissimilar or their fidelity is at most 1/2. Recall that our measure for the transmission quality is the *worst-case* fidelity.

Our Contribution. In this paper, we give a protocol such that for *any* quantum states $|\psi_1\rangle$ at s_1 and $|\psi_2\rangle$ at s_2, $F(|\psi_1\rangle, \boldsymbol{\rho}_1)$ and $F(|\psi_2\rangle, \boldsymbol{\rho}_2)$ are both strictly greater than 1/2 (Theorem 3.1), where F is the fidelity. The idea is discretization of (continuous) quantum states. Namely, the quantum state from s_2 is changed into classical three bits which are used as a key to "encode" the state from s_1 at node s_0 and "decode" it at node t_1. At node t_2, we recover the key bits by comparing the state from s_1 and its encoded one from t_0. For these purposes, we need the above approximated cloning, and what we call "three-dimensional (3D) measurement" that gives us which basis the current quantum state is close to. Moreover, we use "approximated group

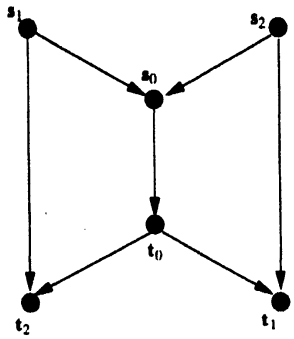

Figure 1: Butterfly network.

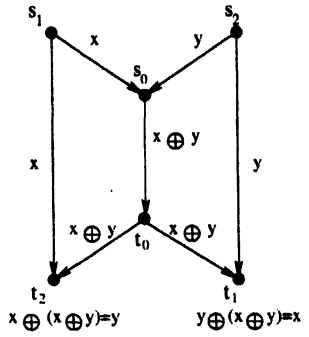

Figure 2: Coding scheme

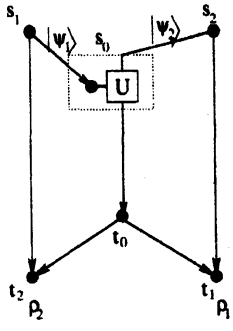

Figure 3: Network using a controlled unitary operation

operations" for encoding quantum states and the Bell measurement for their comparison.

Note that the present value of $F(|\psi_1\rangle, \rho_1)$ and $F(|\psi_2\rangle, \rho_2)$ is only slightly better than $1/2$ (some $1/2 + 1/100$) in general. However, if we impose some restriction, the value becomes much better. For example, if $|\psi_1\rangle$ is a classical state (i.e. either $|0\rangle$ or $|1\rangle$), then the fidelity becomes $2/3$ (Theorem 4.1). Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states, especially if they are so called quantum random access coding states [3]. By using this, we can design an interesting protocol which can send two classical bits from s_1 to t_1 (similarly two bits from s_2 to t_2) but only one of them, determined by adversary, should be recovered. It is shown that the success probability for this protocol is $1/2 + \sqrt{2}/16$ (Theorem 4.2), but classically the success probability for any protocol is at most $1/2$.

Related Work. The study of coding methods on quantum information and computation has been deeply explored for error correction of quantum computation (since [22]) and data compression of quantum sources (since [21]). Recall that their techniques are duplication of data (error correction) and average-case analysis (data compression). Those standard approaches do not seem to help in the core of our problem.

More tricky applications of quantum mechanism are quantum teleportation [5], superdense coding [6], and a variety of quantum cryptosystems including the BB84 key distribution [4]. Probably most related one to this paper is the random access coding by Ambainis, Nayak, Tashma, and Vazirani [3], which allows us to encode two or more classical bits into one qubit and decode it to recover any one of the source bits. Our third protocol is a realization of this scheme on the Butterfly network.

Different from the classical world, the quantum mechanics prohibits us from exact manipulation of some fundamental operations such as cloning a qubit [23], deleting one of two copies of a qubit [20], and the universal NOT of a qubit (on the Bloch sphere) [8]. However, since these operations are so basic ones, it was natural that their approximated or probabilistic versions were investigated. For instance, Bužek and Hillery [9] found a quantum cloning machine which produces two copies of any unknown original state with fidelity $5/6$, which was shown to be optimal [7]. Our approximated approach reflects the policy of these studies on manipulations of unknown quantum states.

In this paper, we omit all the proofs of our results. See [15] for the details.

2 Formal Setting

Our model as a quantum circuit is shown in Fig. 4. The information sources at nodes s_1 and s_2 are pure one-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. (It turns out, however, that the result does not change for mixed states because of the joint concavity of the fidelity [19].) Any node does not have prior entanglement with other nodes. At every node, a physically allowable operation, i.e., trace-preserving completely positive map (TP-CP map), is done, and each edge can send only one qubit. They are implemented by unitary operations with additional ancillae and by discarding all qubits except for the output qubits [1, 19].

Our goal is to send $|\psi_1\rangle$ to node t_1 and $|\psi_2\rangle$ to node t_2 as well as possible. The quality of data at node t_j is measured by the fidelity between the original state $|\psi_j\rangle$ and the state ρ_j output at node t_j by the protocol. Here, the fidelity between two quantum states ρ and σ are defined as $F(\sigma, \rho) = \left(\mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right)^2$ as in [7, 11, 12]. (The other common definition is $\mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$.) In particular, the fidelity between a pure state $|\psi\rangle$ and a mixed state ρ is $F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle$. (To

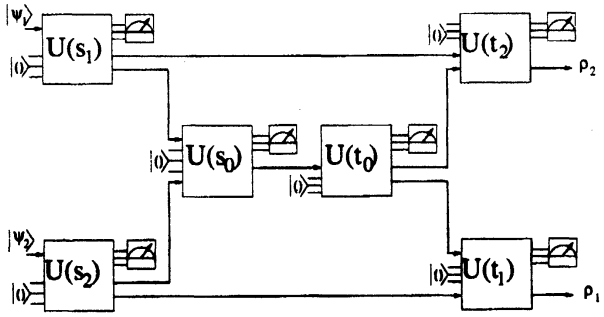

Figure 4: Quantum circuit for coding on the Butterfly network

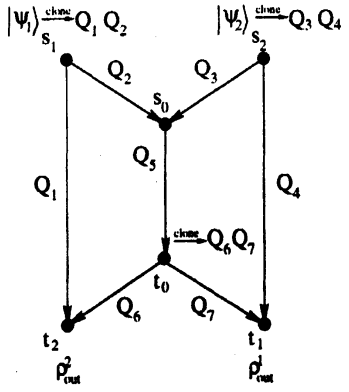

Figure 5: Protocol XQQ.

simplify the description, for a pure state $|\psi\rangle\langle\psi|$ we often use the vector representation $|\psi\rangle$.) We call the minimum of $F(|\psi_j\rangle, \rho_j)$ over all one-qubit states $|\psi_j\rangle$ the *fidelity at node* t_j. Note that a protocol which achieves a fidelity of $1/2$ trivially exists (i.e., the one which outputs completely mixed states at t_1 and t_2 regardless of the input.) So, the question is whether we can achieve a fidelity strictly better than $1/2$.

3 Main Result

In this section we state the following main theorem.

Theorem 3.1 *There exists a quantum protocol whose fidelities at nodes* t_1 *and* t_2 *are* $1/2 + 200/19683$ *and* $1/2 + 180/19683$, *respectively.*

3.1 Overview of the Protocol

Fig. 5 illustrates our protocol, Protocol for Crossing Two Qubits (XQQ). As expected, the approximated cloning is used at nodes s_1, s_2 and t_0.

At node s_0, we first apply the 3D measurement to the state of one-qubit system $\mathcal{Q}_3$ and obtain three classical bits $r_1r_2r_3$. Their different eight values suggest which part of the Bloch sphere the state of $\mathcal{Q}_3$ sits in. These eight values are then used to choose one of eight operations, the approximated group operations, to encode the state of $\mathcal{Q}_2$. These eight operations include identity I, bit-flip X, phase-flip Z, bit+phase-flip Y, and their combination with the universal NOT [10] denoted by Inv. Here, we need to be careful since Inv is not physically allowable. Actually, therefore, we use its approximation $\mathrm{Inv}' = \frac{1}{3}\mathrm{Inv} + \frac{I}{3}$, which turns out to be physically allowable. At node t_1, we apply the reverse operations of these eight operations (actually the same as the original ones) for the decoding purpose.

At node t_2, we recover the three bits $r_1r_2r_3$ (actually the corresponding quantum state for the output state) by comparing $\mathcal{Q}_1$ and $\mathcal{Q}_6$. This should be possible since $\mathcal{Q}_2$ ($\approx \mathcal{Q}_1$) is encoded into $\mathcal{Q}_5$ ($\approx \mathcal{Q}_6$) by using $r_1r_2r_3$ as a key but its implementation is not obvious. It is shown that for this purpose, we can use the Bell measurement together with the fact that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are partially entangled as a result of cloning at node s_1.

4 Protocols for Restricted Problems

4.1 Protocol XQC

We first consider the case where one of the sources (say, node s_2) receives a classical bit b. Notice that, in this case, the fidelity at node t_2 equals to the probability that b can be recovered successfully at t_2. See Fig. 6 for the protocol XQC.

Theorem 4.1 *XQC achieves a fidelity of $2/3$ at both t_1 and t_2.*

As before we use cloning at s_1 and s_2 but there is no shrink at s_2 this time. At s_0, the state on Q_2 is bit-flipped iff $b = 1$. Then, the decoding process is rather straightforward: at t_1 the state is flipped back iff $b = 1$, while at t_2 the quantum states received from s_1 and t_0 are compared to retrieve b by an appropriate measurement. As mentioned in Sec. 1, this protocol would not work if perfect cloning were possible (and were used) at node s_1. The approximated cloning at s_1 creates some entanglement between Q_1 and Q_2 (and between Q_1 and Q_6), which is essential for the performance of XQC.

4.2 Protocol $X2C2C$

We next consider the case that both sources are restricted to be one of the four $(2, 1, \cos^2 \pi/8)$-quantum random access (QRA) coding states [3], where (m, n, p)-QRA coding is the coding of m bits to n qubits such that any one bit chosen from the m bits is recovered with probability p. In this case, we can send them with high fidelity (at least $3/4$) from s_1 to t_1 and from s_2 to t_2 by combining the measurement in the basis B_x at the sources and the classical network coding scheme for the Butterfly network.

As an application, we can consider a more interesting problem where each source receives two classical bits, namely, $x_1x_2 \in \{0,1\}^2$ at s_1, and $y_1y_2 \in \{0,1\}^2$ at s_2. At node t_1, we output one classical bit Out^1 and similarly Out^2 at t_2. Now an adversary chooses two numbers $i_1, i_2 \in \{1,2\}$. Our protocol can use the information of i_1 only at node t_1 and that of i_2 only at t_2. Our goal is to maximize $F(x_{i_1}, \mathrm{Out}^1)$ and $F(y_{i_2}, \mathrm{Out}^2)$, where $F(x_{i_1}, \mathrm{Out}^1)$ turns out to be the probability that $x_{i_1} = \mathrm{Out}^1$ and similarly for $F(y_{i_2}, \mathrm{Out}^2)$. Fig. 7 illustrates $X2C2C$.

Theorem 4.2 *$X2C2C$ achieves a fidelity of $1/2 + \sqrt{2}/16$ at both t_1 and t_2.*

By contrast, any classical protocol cannot achieve a success probability greater than $1/2$ for the following reason: Let fix $y_1 = y_2 = 0$. Then the path from s_1 to t_1 is obviously equivalent to the $(2, 1, p)$-classical random access coding, where the success probability p is at most $1/2$ [3].

References

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. *Proc. 30th ACM STOC*, pp. 20–30, 1998.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory* **46** (2000) 1204–1216.

[3] A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM* **49** (2002) 496–511.

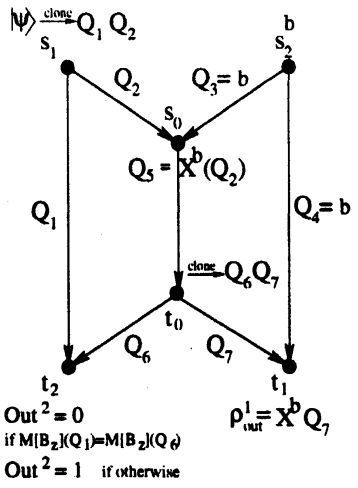

Figure 6: Protocol XQC

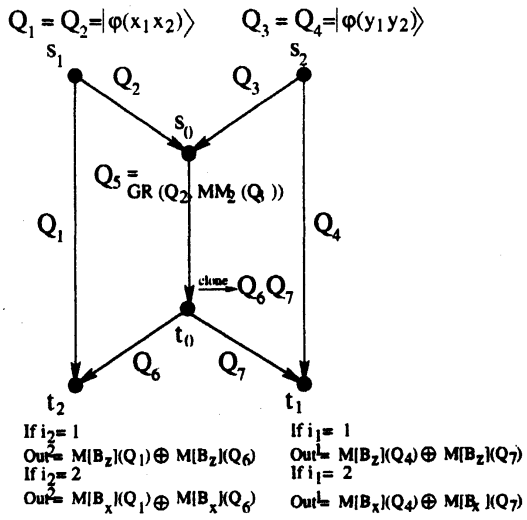

Figure 7: Protocol $X2C2C$

[4] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum states via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70** (1993) 1895–1899.

[6] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69** (1992) 2881–2884.

[7] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin. Optimal universal and state-dependent quantum cloning. *Phys. Rev. A* **57** (1998) 2368–2378.

[8] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello. Phase-covariant quantum cloning. *Phys. Rev. A* **62** (2000) 012302.

[9] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A* **54** (1996) 1844–1852.

[10] V. Bužek, M. Hillery, and R. F. Werner. Optimal manipulation with qubits: universal NOT gate. *Phys. Rev. A* **60** (1999) 2626–2629.

[11] H. Fan, K. Matsumoto, X.-B. Wang, and H. Imai. Phase-covariant quantum cloning. *J. Phys. A: Math. Gen.* **35** (2002) 7415–7423.

[12] N. Gisin and S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.* **79** (1997) 2153–2156.

[13] N. Gisin and S. Popescu. Spin flips and quantum information for antiparallel spins. *Phys. Rev. Lett.* **83** (1999) 432–435

[14] N. J. Harvey, D. R. Karger, and K. Murota. Deterministic network coding by matrix completion. *Proc. 16th ACM-SIAM SODA*, pp. 489–498, 2005.

[15] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Quantum network coding. Available at quant-ph/0601088.

[16] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, L. M. G. M. Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Transactions on Information Theory* **51** (2005) 1973–1982.

[17] A. R. Lehman and E. Lehman. Complexity classification of network information flow problems. *Proc. 15th ACM-SIAM SODA*, pp. 142–150, 2004.

[18] A. R. Lehman and E. Lehman. Network coding: does the model need tuning? *Proc. 16th ACM-SIAM SODA*, pp. 499–504, 2005.

[19] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge, 2000.

[20] A. K. Pati and S. L. Braunstein. Impossibility of deleting an unknown quantum state. *Nature* **404** (2000) 164–165.

[21] B. Schumacher. Quantum coding. *Phys. Rev. A* **51** (1995) 2738–2747.

[22] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52** (1995) 2493–2496.

[23] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature* **299** (1982) 802–803.